Symantec™ Drive Encryption for Linux Version 10.3 Release Notes

Thank you for using this Symantec Corporation product. These Release Notes contain important information regarding this release of Symantec Drive Encryption for Linux. Symantec Corporation strongly recommends you read this entire document.

Symantec Corporation welcomes your comments and suggestions. You can use the information in Getting Assistance to contact us.

Product: Symantec Drive Encryption for Linux

Version: 10.3.0

Warning: Export of this software may be restricted by the U.S. government.

Note: To view the most recent version of this document, go to the Products section on the Symantec Corporation Web site.

About Symantec Drive Encryption for Linux

Symantec Drive Encryption for Linux, Powered by PGP Technology is a software product from Symantec Corporation that locks down the entire contents of your Linux system.

Changes in This Release

This section describes the changes and new features in this release of Symantec Drive Encryption for Linux.

What's New in Symantec Drive Encryption for Linux 10.3

What's New in 10.3.0

- **Symantec identity branding**

  The PGP product line has been renamed. For a detailed map of old product names to new ones, refer to the Symantec Knowledgebase article TECH197084.

- **Compatibility with New Linux Packages**

  This release supports installation of Symantec Drive Encryption for Linux, formerly known as PGP Whole Disk Encryption for Linux, on Red Hat Enterprise Linux/CentOS 6.1 and 6.2 (32-bit and 64-bit versions).

Deprecated Commands or Options

Beginning with 10.2.0, the `--offset` command is deprecated.

System Requirements

Symantec Drive Encryption for Linux runs on these platforms:

- Ubuntu 10.04 LTS; (32-bit and 64-bit versions)
- Red Hat Enterprise Linux/CentOS 5.4, 5.5, 5.6, 5.7, 5.8, 6.0, 6.1, 6.2; (32-bit and 64-bit versions)

Note: Symantec Drive Encryption for Linux runs on the above platforms when all of the latest hot fixes and security patches have been applied.

Note: CentOS is free, open source software based on Red Hat Enterprise Linux. For the purposes of supporting Symantec Drive Encryption for Linux, the two are functionally equivalent.

Note: Symantec Drive Encryption for Linux no longer runs on these platforms: Red Hat Enterprise Linux/CentOS 5.2, Red Hat Enterprise Linux/CentOS 5.3, Ubuntu 9.04.

The system requirements for Symantec Drive Encryption for Linux are:

- Generic Linux kernel. Kernels modified for PAE, Xen, or RT are not supported.
- 512 MB of RAM
- 64 MB hard disk space
- Internet access during installation, except on systems that have the required packages pre-installed or have access to a local repository of packages. For Red Hat Enterprise Linux/CentOS, the required packages are dkms, gcc, make, and patch. For Ubuntu, they are dkms, gcc, make, and libc6-dev. Both platforms also require the development package for the currently running kernel.

Symantec Drive Encryption for Linux is compatible with the default Logical Volume Manager (LVM) installation. That is, for systems using LVM, the /boot directory must reside on a normal (non-LVM) partition. This constraint can be satisfied by one of two ways: (a) The root (/) is a normal (non-LVM) partition; or (b) /boot itself is a mount point for a normal partition.

Installing

Warning: When upgrading an existing installation of Symantec Drive Encryption for Linux that runs on Ubuntu 8.04, decrypt the system's disks before starting the upgrade. When installation is complete, re-encrypt the disks. This warning applies only to systems with partially or fully encrypted system disks. Failure to follow these instructions will result in the loss of encrypted data.

To install Symantec Drive Encryption for Linux

1. Download the installer file to a known location on your system.
2. Open a terminal window, and change the current directory to the directory with the installer file.
3. Extract and install Symantec Drive Encryption for Linux as follows:
   - For Ubuntu, type the following command. When prompted, supply the root password.

     ```
     sudo bash pgp_desktop_10.3.0_linux_ub10.04_i386.bsx
     ```

   - For Red Hat Enterprise Linux, type the following commands. When prompted, supply the root password.

     ```
     su - root

     bash pgp_desktop_10.3.0_linux_ub10.04_i386.bsx
     ```

4. Read and accept the license agreement.
5. Reboot your system when the installation is complete.

For additional information, including upgrade instructions, see the *Symantec Drive Encryption for Linux User's Guide*.

Licensing

Symantec Drive Encryption for Linux requires a valid license to operate.

If you are using Symantec Drive Encryption for Linux in a Symantec Encryption Management Server-managed environment, you do not need to license Symantec Drive Encryption for Linux; the installer includes a license.

If you are using Symantec Drive Encryption for Linux standalone, you must license it with a valid Symantec Encryption Desktop license that includes support for Symantec Drive Encryption.

If you attempt to use Symantec Drive Encryption for Linux standalonewithout entering a license, only basic functionality will be available; you will only be able to view the files on the encrypted drive and decrypt the drive.

Note: You should license Symantec Drive Encryption for Linux immediately after installation, as you cannot encrypt your drive until Symantec Drive Encryption for Linux is licensed.

Use `--license-authorize` to license Symantec Drive Encryption for Linux.

The usage format is:

```
pgpwde --license-authorize --license-name <name> --license-number <number> [--
license-email <emailaddress>] [--license-organization <org>]
```

Where:

- `--license-authorize` is the command to license Symantec Drive Encryption for Linux.
- `--license-name <Name>`

  Where `<Name>` is your name or a descriptive name.

- `--license-organization <Org>`

  Where `<Org>` is the name of your company.

- `--license-number <Number>`

  Where `<Number>` is a valid license number.

For example:

```
pgp --license-authorize --license-name "Alice Cameron" --license-organization
"Example Corporation" --license-number "AAAAA-BBBBB-CCCCC-DDDDD-EEEEE-FFF"
```

This example shows Alice Cameron, a standalone user, licensing Symantec Drive Encryption for Linux.

You can ignore error messages stating that no email address was specified, if you receive one. Including an email address is optional, not required, for license authorization.

Refer to the *Symantec Drive Encryption for Linux User's Guide* for more information about licensing.

Enrolling

You must enroll Symantec Drive Encryption for Linux after installation if you are using it in a Symantec Encryption Management Server-managed environment.

After enrolling, Symantec Drive Encryption for Linux will receive policies and settings from its Symantec Encryption Management Server. It will also send information to the Symantec Encryption Management Server that can be seen by the Symantec Encryption Management Server administrator.

Note: You must initiate enrollment on your own. You will not be prompted to do so.

Enrollment uses LDAP credentials. The username and passphrase required for both enrolling and checking enrollment status are the username and passphrase of the user on the LDAP server.

Use `--enroll` to enroll Symantec Drive Encryption for Linux.

Note: `--enroll` is preceded by **pgpenroll** instead of the usual **pgpwde**.

The usage format is:

```
pgpenroll --enroll [--username <user>] [--passphrase <phrase>]
```

Where:

- `--enroll` is the command to enroll with a Symantec Encryption Management Server.
- `--username` specifies a username for an operation (optional).

  `<user>` is the username (on the LDAP server) of the user being enrolled.

- `--passphrase` specifies the passphrase for an operation (optional).

  `<phrase>` is the passphrase (on the LDAP server) of the user being enrolled.

Example:

```
pgpenroll --enroll --username "Alice Cameron"
--passphrase 'Frodo@Baggins22'
```

This example shows user Alice Cameron enrolling Symantec Drive Encryption for Linux. The username and passphrase she is using are her credentials on her organization's LDAP server.

Refer to the *Symantec Drive Encryption for Linux User's Guide* for more information about enrolling.

Additional Information

This section includes important information about using Symantec Drive Encryption for Linux.

- **Mounting or unmounting the USB Drive** - For the safety of your USB device, ensure that you mount or unmount the device properly before you encrypt or decrypt the device.
- **Upgrading when multiple PGP client products are installed.** If both client and command-line products are installed on the same system and those versions are earlier than 10.2, you must upgrade both products at the same time. If only one product is updated to version 10.2 or later, then the other product will not function correctly until it is also updated. [31379/2476336]
- **Limitations with Logical Volume Manager (LVM) with RAID.** Systems that use LVM with RAID are incompatible with Symantec Drive Encryption. [nbn]
- **PGP BootGuard background cannot be changed to an image.** Calling the `--set-background` command with an image changes the background to black. The provided image is not visible in the PGP BootGuard background. [25401/2470353]
- **Incomplete encryption of disks that are partitioned with Acronis.** Symantec Drive Encryption does not encrypt external disks that are formatted and partitioned with Acronis Disk Director. [30827/2475784]
- **Passphrase required for stop command.** The `--stop` command now requires a passphrase. Scripts that use this command without providing a passphrase will fail. [29822/2474778]
- **Domain required for Symantec Drive Encryption command line recovery-configure command.** The `--recovery-configure` command now requires a domain for users that have one. In these situations, scripts that use this command without providing a domain will fail. [28656/2473612]
- **NTFS-formatted disks.** Symantec Drive Encryption for Linux, in most cases, is compatible with NTFS-formatted disks provided you have the appropriate drivers (NTFS-3G, for example) installed for reading and writing to NTFS-formatted disks. [26471/2471425]

Before mounting an encrypted NTFS-formatted disk, you must first authenticate to the disk. To do this,first use the `--enum` command to determine the disk number of the NTFS-formatted disk:

```
pgpwde --enum
```

Then authenticate to the NTSF-formatted disk:

pgpwde --auth --disk <disknumber> --passphrase <auth-passphrase>

- **Uninstalling or removing packages.** For systems that are encrypted with Symantec Drive Encryption, decrypt any encrypted drives *before* uninstalling Symantec Drive Encryption for Linux or removing any packages. [25780/2470733]
- **Multi-boot systems.** Your system may not boot correctly after being encrypted if the operating system does not reside on the same disk as the boot loader. To resolve this issue, make sure to mount the correct /boot partition on all of your Linux installs. [25099/2470051]

Getting Assistance

Available Documentation

Documentation for Symantec Drive Encryption for Linux includes a help page in HTML format and the *Symantec Drive Encryption for Linux User's Guide* (in PDF format) for all supported platforms. Both the help page and the user's guide are included in the release package. You can view and print the user's guide with Adobe Acrobat Reader, available on Adobe's Web site.

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, Africa	semea@symantec.com
North America, Latin America	supportsolutions@symantec.com

Copyright and Trademarks